(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（A）　(11)特許出願公開番号

特開平11－213553

(43)公開日　平成11年(1999)８月６日

(51)Int.Cl.[6]		識別記号	FI		
Ｇ１１Ｂ	20/10		Ｇ１１Ｂ	20/10	Ｈ
Ｇ０９Ｃ	1/00	６４０	Ｇ０９Ｃ	1/00	６４０Ｚ
Ｈ０４Ｌ	9/32		Ｈ０４Ｌ	9/00	６７３Ｂ

審査請求　未請求　請求項の数５　ＯＬ　（全 12 頁）

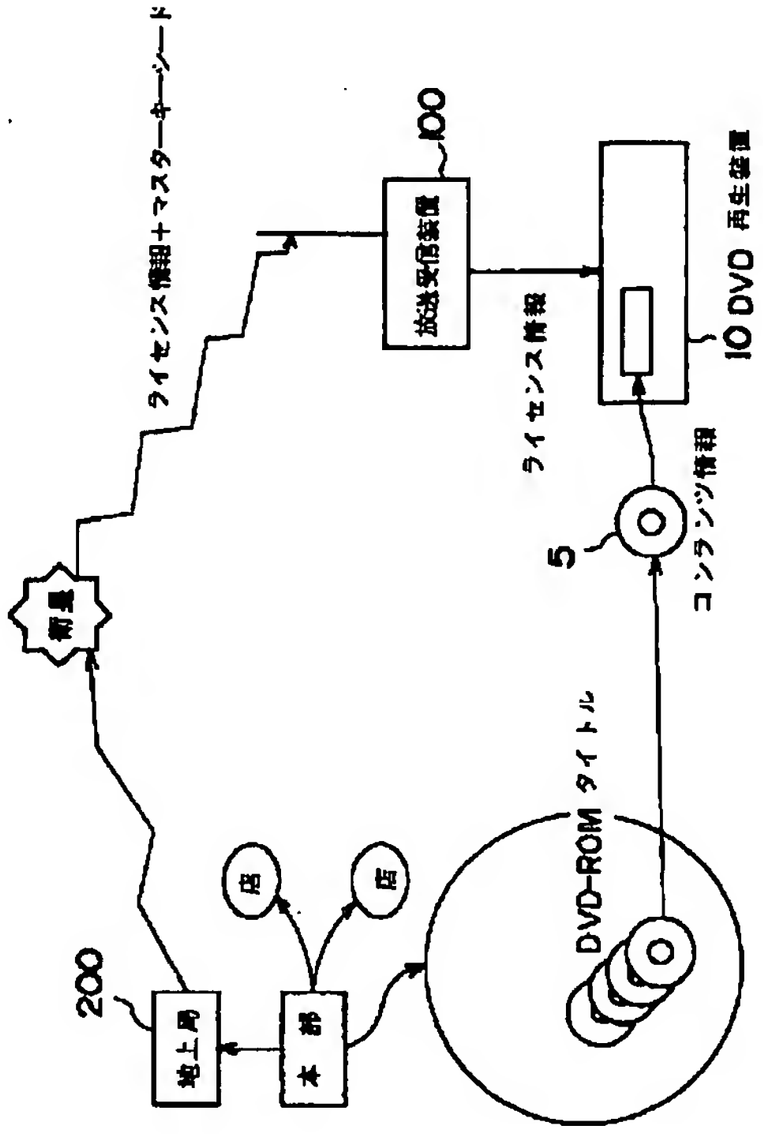
(21)出願番号　特願平10－15788

(22)出願日　平成10年(1998)１月28日

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地
(72)発明者　上林　達
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内
(72)発明者　秋山　浩一郎
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内
(72)発明者　辻本　修一
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内
(74)代理人　弁理士　鈴江　武彦　（外６名）

(54)【発明の名称】　契約管理装置および再生装置

(57)【要約】
【課題】ディジタル化された著作物を迅速かつ手軽に流通させるとともに、ディジタル化された著作物の視聴の契約に基づく著作権の保護を前提としたディジタル情報の利用環境を提供する情報流通システムを提供する。
【解決手段】記録媒体に記録された暗号化されたコンテンツ情報を再生する再生装置を視聴契約に基づき放送にて制御するための契約管理装置であって、個々のコンテンツ情報のそれぞれに対応付けられた少なくとも暗号化された該コンテンツ情報を復号する第１の鍵情報と前記再生装置の識別情報とを含む暗号化された制御情報と、前記暗号化された制御情報を復号する第２の鍵情報を生成するために必要な鍵生成情報とを放送配信する手段を具備し、前記制御情報に含まれる識別情報にて特定される再生装置に対してのみ該制御情報に基づくコンテンツ情報の再生が許可されることを特徴とする。



【特許請求の範囲】
【請求項１】　記録媒体に記録された暗号化されたコンテンツ情報を再生する再生装置を視聴契約に基づき放送にて制御するための契約管理装置であって、
個々のコンテンツ情報のそれぞれに対応付けられた少なくとも暗号化された該コンテンツ情報を復号する第１の鍵情報を含む暗号化された制御情報と、該暗号化された制御情報を復号する第２の鍵情報を生成するために必要な鍵生成情報とを放送配信する手段を具備し、
視聴契約に基づき放送波の受信動作を制御するために配信される信号にて、前記再生装置の再生動作を制御することを特徴とする契約管理装置。
【請求項２】　記録媒体に記録された暗号化されたコンテンツ情報を再生する再生装置を視聴契約に基づき放送にて制御するための契約管理装置であって、
個々のコンテンツ情報のそれぞれに対応付けられた少なくとも暗号化された該コンテンツ情報を復号する第１の鍵情報と前記再生装置の識別情報とを含む暗号化された制御情報と、前記暗号化された制御情報を復号する第２の鍵情報を生成するために必要な鍵生成情報とを放送配信する手段を具備し、
前記制御情報に含まれる識別情報にて特定される再生装置に対してのみ該制御情報に基づくコンテンツ情報の再生が許可されることを特徴とする契約管理装置。
【請求項３】　前記鍵生成情報は、所定期間毎に更新されることを特徴とする請求項１または２記載の契約管理装置。
【請求項４】　放送配信された、個々のコンテンツ情報のそれぞれに対応付けられた少なくとも暗号化された該コンテンツ情報を復号する第１の鍵情報を含む暗号化された制御情報と、該暗号化された制御情報を復号する第２の鍵情報を生成するために必要な鍵生成情報とに基づき、記録媒体に記録された暗号化されたコンテンツ情報を再生する再生装置であって、
前記鍵生成情報に基づき生成された第２の鍵情報を用いて前記暗号化された制御情報を復号する復号手段と、
この復号手段で復号された制御情報に含まれる第１の鍵情報を用いて前記記録媒体に記録された暗号化されたコンテンツ情報を復号再生する再生手段と、
を具備し、
前記再生手段は、視聴契約に基づき放送波の受信動作を制御するために配信される信号にて制御されることを特徴とする契約管理装置。
【請求項５】　放送配信された、個々のコンテンツ情報のそれぞれに対応付けられた少なくとも暗号化された該コンテンツ情報を復号する第１の鍵情報と前記再生装置の識別情報とを含む暗号化された制御情報と、前記暗号化された制御情報を復号する第２の鍵情報を生成するために必要な鍵生成情報とに基づき、記録媒体に記録された暗号化されたコンテンツ情報を再生する再生装置であって、
前記鍵生成情報に基づき生成された第２の鍵情報を用いて前記暗号化された制御情報を復号する復号手段と、
この復号手段で復号された制御情報に含まれる第１の鍵情報を用いて前記記録媒体に記録された暗号化されたコンテンツ情報を復号再生する再生手段と、
を具備し、
前記再生手段は、前記制御情報に含まれる前記識別情報により前記コンテンツ情報の再生の可否を判断することを特徴とする契約管理装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、例えばＤＶＤ等の記録媒体にて暗号化されたコンテンツ情報を顧客に（有料）配布し、例えば衛星放送にてコンテンツ情報の復号鍵情報を含む制御情報を再生装置に配信して、そのコンテンツ情報の視聴契約（例えば、視聴期間）に応じて視聴可能にする情報流通システムに関する。
【０００２】
【従来の技術】近年、ディジタル情報処理技術や広帯域ＩＳＤＮ等の通信技術の発達、ＤＶＤ等の大容量、高画質、高音質を実現する高度な情報記録媒体の開発が進んでいる。このような情報の伝達手段の多様化、高度化が進むにつれ、ディジタル化された著作物等がネットワーク、記録媒体などを介して利用者の手元に大量に頒布され、利用者がそれらを自由に利用できる環境が生まれつつある。このような環境は、著作物の無断複製、無断改変、著作者の意図しない流通などが起こる機会を増大させるものであり、著作物の権利者にとって、自己の利益が不当に害されるのではないかという懸念を抱かせるものである。
【０００３】このような著作物の権利者の懸念を拭い払えるよう、迅速かつ手軽にディジタル化された著作物を流通させるとともに、適正にそれらを利用できるようなディジタル情報の利用環境を提供できる著作権の保護を前提としたシステムの開発は今後の重要な課題となる。
【０００４】ＤＶＤは、ＣＤ－ＲＯＭに代わる大容量のパソコンメディアであるとともに、映画、音楽、ゲーム、カラオケ等、様々な用途への広がりを期待でき、このようなＤＶＤの普及を図るために、ＤＶＤのタイトル価格を低く抑えたり、レンタルＤＶＤ市場への拡大も予想される。従って、このような観点からも、ＤＶＤ等の記録媒体に記録されたディジタル化された著作物の所有ではなく利用に対して課金するという考えに基づく、情報に対する著作権の保護を前提とした情報の流通システムが不可欠となる。
【０００５】一方、ディジタル放送は、通信衛星（ＣＳ）に始まって、ケーブルＴＶ、地上放送へとディジタル化が進むにつれ、いっそうのサービスの充実が期待されており、これからの放送サービスの主役をつとめてい

くものと思われる。
【０００６】ディジタル放送の最大の特徴は、情報圧縮技術の導入により、番組の送信に要する周波数の使用効率の向上が図れ、アナログ放送に比較して放送チャネル数の大幅な増加が可能となったことである。さらに、高度な誤り訂正技術が適用でるため、高品質で均質なサービスの提供が可能となる。
【０００７】放送のディジタル化により、多様な情報形態（映像、音声、文字、データ等）によるマルチメディアサービスの提供が可能となり、そのようなサービスを提供するためのシステムも続々登場してきている。
【０００８】このようなシステムで、契約内容に基づいてスクランブルを解く、あるいは復号する有料放送サービスを提供する際、契約期間に即した顧客管理が行えなければいけない。契約期間に即した顧客管理とは、例えば、所定の料金の支払により契約された契約期間内に限って契約チャネルの番組の視聴を可能とするというものである。
【０００９】また、受信装置にてスクランブルあるいは暗号を解くための鍵情報は、不正視聴を防止する上からも正当な視聴者のみに（契約チャネル、契約期間に即して）しかも確実に提供する必要がある。
【００１０】
【発明が解決しようとする課題】そこで、本発明は、ディジタル化された著作物を迅速かつ手軽に流通させるとともに、ディジタル化された著作物の視聴の契約に基づく著作権の保護を前提としたディジタル情報の利用環境を提供する情報流通システムを提供することを目的とする。
【００１１】本発明は、記録媒体に記録された暗号化されたコンテンツ情報を再生する再生装置を視聴契約に基づき放送にて制御するための契約管理装置であって、ＤＶＤ等の記録媒体に記録されたコンテンツ情報を再生する再生装置を視聴契約に基づき放送にて制御でき、ＤＶＤ等の記録媒体に記録されたディジタル化された著作物（コンテンツ情報）の視聴を契約期間に限って視聴可能にすることができる契約管理装置を提供することを目的とする。
【００１２】また、本発明は、放送配信される制御情報に基づき、ＤＶＤ等の記録媒体に記録された暗号化されたコンテンツ情報の再生を当該コンテンツ情報の視聴契約期間に限って可能にすることがきる再生装置を提供することを目的とする。
【００１３】
【課題を解決するための手段】本発明の契約管理装置は、記録媒体に記録された暗号化されたコンテンツ情報を再生する再生装置を視聴契約に基づき放送にて制御するための契約管理装置であって、個々のコンテンツ情報のそれぞれに対応付けられた少なくとも暗号化された該コンテンツ情報を復号する第１の鍵情報を含む暗号化された制御情報と、該暗号化された制御情報を復号する第２の鍵情報を生成するために必要な鍵生成情報とを放送配信する手段を具備し、視聴契約に基づき放送波の受信動作を制御するために配信される信号にて、前記再生装置の再生動作を制御することにより、ＤＶＤ等の記録媒体に記録されたコンテンツ情報を再生する再生装置を視聴契約に基づき放送にて制御でき、ＤＶＤ等の記録媒体に記録されたディジタル化された著作物（コンテンツ情報）の視聴を契約期間に限って視聴可能にすることができる。
【００１４】また、本発明の契約管理装置は、記録媒体に記録された暗号化されたコンテンツ情報を再生する再生装置を視聴契約に基づき放送にて制御するための契約管理装置であって、個々のコンテンツ情報のそれぞれに対応付けられた少なくとも暗号化された該コンテンツ情報を復号する第１の鍵情報と前記再生装置の識別情報とを含む暗号化された制御情報と、前記暗号化された制御情報を復号する第２の鍵情報を生成するために必要な鍵生成情報とを放送配信する手段を具備し、前記制御情報に含まれる識別情報にて特定される再生装置に対してのみ該制御情報に基づくコンテンツ情報の再生が許可されることにより、ＤＶＤ等の記録媒体に記録されたコンテンツ情報を再生する再生装置を視聴契約に基づき放送にて制御でき、ＤＶＤ等の記録媒体に記録されたディジタル化された著作物（コンテンツ情報）の視聴を契約期間に限って視聴可能にすることができる。
【００１５】本発明の再生装置は、放送配信された、個々のコンテンツ情報のそれぞれに対応付けられた少なくとも暗号化された該コンテンツ情報を復号する第１の鍵情報を含む暗号化された制御情報と、該暗号化された制御情報を復号する第２の鍵情報を生成するために必要な鍵生成情報とに基づき、記録媒体に記録された暗号化されたコンテンツ情報を再生する再生装置であって、前記鍵生成情報に基づき生成された第２の鍵情報を用いて前記暗号化された制御情報を復号する復号手段と、この復号手段で復号された制御情報に含まれる第１の鍵情報を用いて前記記録媒体に記録された暗号化されたコンテンツ情報を復号再生する再生手段と、を具備し、前記再生手段は、視聴契約に基づき放送波の受信動作を制御するために配信される信号にて制御されることにより、放送配信されるライセンス情報に基づき、ＤＶＤ等の記録媒体に記録された暗号化されたコンテンツ情報の再生を当該コンテンツ情報の視聴契約期間に限って可能にすることがきる。
【００１６】また、本発明の再生装置は、放送配信された、個々のコンテンツ情報のそれぞれに対応付けられた少なくとも暗号化された該コンテンツ情報を復号する第１の鍵情報と前記再生装置の識別情報とを含む暗号化された制御情報と、前記暗号化された制御情報を復号する第２の鍵情報を生成するために必要な鍵生成情報とに基

づき、記録媒体に記録された暗号化されたコンテンツ情報を再生する再生装置であって、前記鍵生成情報に基づき生成された第２の鍵情報を用いて前記暗号化された制御情報を復号する復号手段と、この復号手段で復号された制御情報に含まれる第１の鍵情報を用いて前記記録媒体に記録された暗号化されたコンテンツ情報を復号再生する再生手段と、を具備し、前記再生手段は、前記制御情報に含まれる前記識別情報により前記コンテンツ情報の再生の可否を判断することにより、放送配信されるライセンス情報に基づき、ＤＶＤ等の記録媒体に記録された暗号化されたコンテンツ情報の再生を当該コンテンツ情報の視聴契約期間に限って可能にすることがきる。

【００１７】

【発明の実施の形態】以下、本発明の実施形態について図面を参照して説明する。

（１）情報流通サービスの概要

図１は、本発明の実施形態に係る情報流通サービスを提供するためのシステム構成例を示したものである。ディジタル化された著作物（例えば映画等）としてのコンテンツ情報は暗号化されて例えばＤＶＤ－ＲＯＭ等の記録媒体（以下、ＤＶＤ－ＲＯＭの場合を例にとり説明する）５に記録されて、例えばレンタル事業会社を介して配布される。

【００１８】レンタル事業会社の本部は、系列各店舗に例えば１タイトル毎の暗号化されたコンテンツ情報の記録されたＤＶＤ－ＲＯＭを配布する。顧客は所望のタイトルのコンテンツ情報の記録されたＤＶＤ－ＲＯＭを購入しただけでは該コンテンツ情報を視聴することはできない。ＤＶＤ－ＲＯＭに記録された暗号化されたコンテンツ情報を復号、再生するための鍵情報（以下、コンテンツキー）が必要である。このコンテンツキーは、暗号化されて、例えばレンタル会社の本部と提携している衛星放送局２００から衛星放送にて各顧客が有する受信装置１００に配信される。

【００１９】顧客は系列店舗にて該コンテンツ情報のＤＶＤ－ＲＯＭを購入した際に、少なくとも視聴期間を定めた視聴契約に応じた料金を支払う。この視聴契約に基づき顧客が有するＤＶＤ－ＲＯＭの再生装置１０にて当該ＤＶＤ－ＲＯＭに記録されたコンテンツ情報を顧客が視聴できるようにすることが本発明の目的とするところである。

【００２０】なお、ＤＶＤ－ＲＯＭに記録された暗号化されたコンテンツ情報を復号するコンテンツキーは、具体的には（以下の説明では）、衛星放送にて配信される一部暗号化されたライセンス情報（後述）に含まれていている。

【００２１】ライセンス情報は、本実施形態の場合、例えば、レンタル会社の本部に設置されている契約管理装置にて生成される。顧客が有する再生装置１０には、受信装置１００（既存のものであることが望ましい）にて受信された衛星放送にて配信されるライセンス情報が入力し、例えば、別途衛星放送にて配信されるマスターキーシードに基づき生成されたマスタキーにて該ライセンス情報の暗号化部分を復号し、所定の判定処理（詳細は後述する）を実行して、当該顧客の行った視聴契約の有効範囲内での該コンテンツ情報の視聴が可能であると判断したときは、当該ライセンス情報に含まれるコンテンツキーを用いてＤＶＤ－ＲＯＭに記録された暗号化されたコンテンツ情報を復号し、再生するようになっている。逆に、再生装置１０に有効なライセンス情報を入力しなければＤＶＤ－ＲＯＭに記録された暗号化されたコンテンツ情報を復号することはできない。

【００２２】衛星放送にて配信されたライセンス情報は、各放送受信装置１００にて受信される。すなわち、本発明の情報流通サービスを利用しようとする顧客は、例えば、従来からある衛星放送の受信サービスを受ける場合と同様、予め当該衛星放送の受信契約を結んでいなければならない。さもなくば、放送受信装置１００にてライセンス情報を正しく取得することができない。

【００２３】放送受信装置１００にて受信されたライセンス情報は、再生装置１０へ送られるようになっている。再生装置１０は、入力されたライセンス情報を、再生装置機内部のライセンス情報蓄積部に保存する。

【００２４】ライセンス情報は、適当なスケジュールに従って、繰り返して放送されている場合がある。このスケジュール方式については後述する。ライセンス情報には、当該ライセンス情報の有効期限情報を含んでいてもよい。

【００２５】次に、本発明に係る情報流通サービスの概要を説明する。本発明に係る情報流通サービスを利用しようとする顧客は、このサービスに適応するＤＶＤ再生装置１０を購入し、さらに、該情報流通サービスを提供している事業会社の系列店舗から所望のタイトルのコンテンツ情報の記録されたＤＶＤ－ＲＯＭを取得するものとする。

【００２６】ＤＶＤ－ＲＯＭには、例えば、図２に示すように、暗号化されたコンテンツ情報が記録されている。所望のタイトルのコンテンツ情報の記録されたＤＶＤ－ＲＯＭを購入しても、該コンテンツ情報が暗号化されているため、そのままでは視聴することはできない。従って、このコンテンツ情報の記録されたＤＶＤ－ＲＯＭを購入する際には、必ずしも著作権相当量の料金を支払う必要が無い。すなわち、本発明に係る情報流通サービスを利用しようとする顧客は、例えば、「ＤＶＤ－ＲＯＭそのものの価格＋手数料」程度のきわめて低価格でＤＶＤ－ＲＯＭを取得することが可能となる。

【００２７】顧客は、購入した当該ＤＶＤ－ＲＯＭをＤＶＤ再生装置１０に挿入し、再生を指示すると、ＤＶＤ再生装置１０のライセンス情報蓄積部から、当該コンテンツ情報にＩＤに一致するライセンス情報を検索する。

初期のライセンス情報が存在しなければ、当該ＤＶＤ－ＲＯＭからコンテンツ情報の再生は行われない。当該コンテンツＩＤに対応するライセンス情報が存在する場合、ＤＶＤ再生装置１０は、ライセンス情報の有効性をチェックする。有効期限が経過しているなど、ライセンス情報が有効でない場合、ＤＶＤ再生装置１０は当該コンテンツ情報の復号再生を行わない。一方、ライセンス情報が有効であれば、ＤＶＤ再生装置１０は、当該コンテンツ情報の復号、再生を行う。

【００２８】このように、顧客のコンテンツ情報の視聴に対する課金（すなわち、著作権相当量の料金）は、衛星放送の受信契約料によって置き換えられる。情報流通サービスを利用しようとする顧客は、先ず、放送受信契約を結び、例えば、月々一定金額の受信料を支払う。次に、受信契約者はレンタル事業会社の系列店舗で、お好みのタイトルのコンテンツ情報を選ぶ。既に述べたように、暗号化コンテンツが記録された記録媒体の取得には、「記録媒体そのものの価格＋手数料」程度の金額を支払えばよい。その後、顧客は持ち帰ったコンテンツ情報をＤＶＤ再生装置１０で受信契約に応じて自由に再生することができる。放送受信装置１００からＤＶＤ再生装置１０に、最新の有効なライセンス情報が供給されているからである。

【００２９】例えば、ライセンス情報の放送配信によって、７月７日２３時５９分迄に配信されるライセンス情報（例えばコンテンツＩＤ「＃２１２４３」のコンテンツ情に対応するもの）は７月１４日２３時５９分と言う有効期限を持つとする。コンテンツＩＤ「＃２１２４３」のコンテンツ情報に対応するライセンス情報で、７月２１日２３時５９分と言う有効期限を有するものは、７月８日０時００分以降７月１４日２３時５９分迄に放送され、ＤＶＤ再生装置１０に格納される。これにより、顧客はコンテンツＩＤ「＃２１２４３」のコンテンツ情報を何時でも再生することができる。

【００３０】さて、当該放送の受信契約者が７月２２日付けで受信契約を解除する場合、契約解除の旨を７月１４日までにレンタル事業会社に通知する。然らば、当該顧客の受信装置１００は７月１４日２３時５９分を以ってライセンス放送の受信を中止する。この場合、７月１５日０時００分以降に放送される、有効期限７月２８日２３時５９を有するＩＤ「＃２１２４３」のライセンス情報は当該受信装置１００に配信されず、当該顧客のＤＶＤ再生装置１０に蓄積されることはない。

【００３１】従って、当該顧客は７月２１日２３時５９分以降は、ＩＤ「＃２１２４３」のコンテンツ情報を視聴できなくなる。以下、より具体的に本発明に係る情報流通サービスを提供するシステムについて説明する。

【００３２】ＤＶＤ－ＲＯＭには、図２に示すように、コンテンツキーにて暗号化されたコンテンツ情報と、該コンテンツ情報の識別情報（コンテンツＩＤ）と、該コンテンツ情報の内容を紹介するプロモーション用の情報とが記録されている。コンテンツＩＤとプロモーション用の情報とは暗号化されていない。なお、コンテンツキーは、各コンテンツ情報毎に異なる。また、コンテンツＩＤは、例えば、タイトル毎に１つづつ付与されているものとする。さらに、コンテンツキーはタイトル毎に予め定められたものである。

【００３３】図３は、ライセンス情報のデータ形式を具体例を示したもので、（ａ）図は、ライセンス情報に受信契約のなされた顧客の有する再生装置のそれぞれを識別するための識別情報（端末ＩＤ）を含まない場合のライセンス情報であり、（ｂ）図は当該ライセンス情報を受けとる再生装置を限定するための端末ＩＤを含む場合のライセンス情報を示している。

【００３４】図３（ａ）に示すライセンス情報は、コンテンツ情報の各タイトル毎に１つづつ生成されるもので、少なくとも当該タイトルのコンテンツＩＤ、コンテンツキーが含まれている。コンテンツＩＤは暗号化されず、それ以外の情報（少なくともコンテンツキー）はマスターキーにて暗号化されている。

【００３５】図３（ａ）に示したようなライセンス情報を用いる場合、顧客毎の視聴期間の管理は、例えば、従来からの衛星放送の受信契約管理の場合と同様、各放送受信装置１００に対し放送波受信可否を制御するための信号（ＯＮ／ＯＦＦ信号）を送ることにより行ってもよい。すなわち、例えば、顧客の視聴期間の開始時に当該顧客の放送受信装置１００に対しＯＮ信号を放送配信し、視聴期間の終了時に当該顧客の放送受信装置１００に対しＯＦＦ信号を放送配信する。放送受信装置１００が当該放送受信装置に対して配信されたＯＮ信号を受信することで放送波の受信を開始し、ＯＦＦ信号を受信することで放送波の受信を不可とする制御を行うようになっている。

【００３６】図３（ｂ）に示すライセンス情報は、少なくとも当該タイトルのコンテンツＩＤ、コンテンツキーと、当該ライセンス情報を受けとる再生装置を特定する端末ＩＤが含まれている。コンテンツＩＤは暗号化されず、それ以外の情報（少なくともコンテンツキー、端末ＩＤ）はマスターキーにて暗号化されている。

【００３７】なお、図３（ｂ）に示すライセンス情報は、端末ＩＤとして、単に個々の再生装置の端末ＩＤを１つのみ記載して、各顧客毎に当該ライセンス情報を生成、配信してもよいし、例えば端末ＩＤの下数桁を端末ＩＤとして記載して、１度に複数の再生装置が受け取れるようにしてもよい。後者の方がライセンス情報の配信効率がよいことは言うまでもない。

【００３８】図３（ｂ）に示すライセンス情報を用いる場合、顧客毎の視聴期間の管理は、例えば、ライセンス情報の端末ＩＤに契約期間がきれた顧客の再生装置１０の端末ＩＤを記載しないことで行うことができる。この

場合、再生装置１０のそれぞれがライセンス情報に含まれる端末ＩＤと自身の端末ＩＤとを比較してライセンス情報を取り込むか否かをチェックすることになる。契約期間中は自身の端末ＩＤそのもが記載された、あるいは自身の端末ＩＤを含むライセンス情報が頻繁に配信されるが、契約期間がきれた時点からライセンス情報には自身の端末ＩＤは記載されなくなる。従って、再生装置１０は、有効なライセンス情報を得られないがためにＤＶＤ－ＲＯＭに記録された暗号化されたコンテンツ情報の復号、再生が行えないことになる。

【００３９】ライセンス情報の暗号化には、次の様な特徴を持った暗号化方式を利用することが望ましい。

１）コンテンツＩＤ、コンテンツキーなどのデータを適当な順序で並べる。ここで、各データをフィールドと呼ぶことがある。

【００４０】２）　適当なアルゴリズムに従って、１）のビット列の順序を攪乱する。この際、広い範囲でビット攪乱が行われることが望ましい。

３）　２）のデータを適当な鍵と暗号方式で暗号化する。１）をそのまま暗号化しないのは、次の理由による。すなわち、通常の暗号方式は、あらかじめ定められた適当なビット長毎に暗号化を行うことを繰り返す。従って、２）の攪乱を行うことにより、ライセンス情報の各フィールドが分離・改変される危険性を低下させることが可能である。

【００４１】（２）契約管理装置

図４は、本実施形態に係る契約管理装置の構成例を示したもので、図１の地上局２００に設置されて用いられる。

【００４２】地上局２００は、図３（ａ）あるいは図３（ｂ）に示したようなライセンス情報とマスターキーシードを放送配信する。ライセンス情報中、コンテンツＩＤ以外の部分はマスターキーにて暗号化されている。ライセンス情報の機密性の向上のためにマスターキーは一定期間毎に更新することが好ましい。そのために、再生装置１０にてマスターキーを生成するために必要な情報、すなわち、マスターキーシードを（定期的あるいはマスターキー更新時に）放送配信するようになっている。

【００４３】さて、図４の契約管理装置は、ライセンス情報の生成、暗号化を行って放送配信するためのものである。顧客との間で放送受信契約がなされると、その契約内容（コンテンツＩＤ、視聴期間等）が、契約ユーザデータベース（ＤＢ）１に登録される。

【００４４】契約ユーザＤＢ１には、図５に示す形式でデータが蓄えられる。図５おいて受端末ＩＤは顧客の有する再生装置１０の端末ＩＤであり、この端末ＩＤに対応させて視聴契約のなされたコンテンツＩＤと視聴期間とが予め定められた形式で記憶されている。

【００４５】シードデータベース（ＤＢ）３は、マスターキー生成用のマスターキーシードから生成されるマスターキーをそのシードＩＤ及び有効期限とともに、図６に示す形式で格納している。シードＤＢ３にはシードＩＤに対応するマスターキーシードも格納されていてもよい。

【００４６】コンテンツキーデータベース（ＤＢ）４は、タイトル毎のコンテンツキーをコンテンツＩＤに対応させて図７に示す形式で格納している。次に、図３（ｂ）に示したようなライセンス情報を生成し、これを放送装置１３を使って受信装置に送る手順を図８に示すフローチャートを参照して説明する。

【００４７】ライセンス情報生成制御部９は、ライセンス情報生成部８に対し、ライセンス情報生成の指示を送る（ステップＳ１１）。この指示とは、例えば「１９９７年１２月１日から１ヶ月間契約している契約ユーザのライセンス情報を送れ」なる内容のもので、予め定められた形式のビット列で表現されたものでもよい。このような指示が出されるとライセンス情報生成部８では契約ユーザＤＢ１から１９９７年１２月１日から少なくとも１ヶ月間契約しているユーザ情報（図５参照）を検索して、当該情報を読み込む（ステップＳ１２～ステップＳ１３）。

【００４８】ここで、契約期間の最小単位は１ヶ月で、契約有効期限は１日にはじまり月末に終了するとし、マスターキーもこの契約最小期間に固有なものとする。すなわち、１１月のマスターキーは１２月のそれとは異なるものを用い、それぞれの月内では変更しないものとする。

【００４９】次に、付加情報生成部８は、コンテンツキーＤＢ４からコンテンツＩＤ毎のコンテンツキーを検索し（ステップＳ１５）、また、シードＤＢ３から１９９７年１２月１日から１９９７年１２月３１日に有効なシードに対応したマスターキーを検索する（ステップＳ１６）。

【００５０】以上によって得られた情報（コンテンツＩＤ、該コンテンツＩＤに対応するコンテンツキー、各ユーザの契約内容）をもとに、付加情報生成部８では、図３（ｂ）に示すようなライセンス情報を生成し、コンテンツＩＤ以外の情報を暗号化する（ステップＳ１７）。ここで生成されたライセンス情報は順次付加情報生成制御部９、放送装置１３に送られる。

【００５１】放送装置１３は、ライセンス情報を所定の周波数帯域の放送波に変換して受信装置に向けて放送配信する（ステップＳ１８）。スケジューリング部１４は、ライセンス情報ＤＢ５に格納されたライセンス情報を配信する際、あるいは、マスターキーシードを配信する際、各ユーザ側の受信装置にて確実にライセンス情報、マスターキーシードが受信されるように配信制御を行うものである。

【００５２】すなわち、例えば、受信契約後、契約変更

時、契約解約時、および、人気のタイトルのコンテンツＩＤに対するライセンス情報を送信する際には、当該ライセンス情報を頻繁に送る必要があり、そのためのライセンス情報の配信スケジューリングに従って、ライセンス情報の配信制御を行うのが、スケジューリング部１４である。

【００５３】ライセンス情報生成部８にて生成されたライセンス情報には、配信日時を示すタイムスタンプが含まれていてもよい。タイムスタンプの示す日時は時計１５にて計時されたできる限り正確なものであり、また、再生装置１０からは各種判定処理に用いる基準となる時刻となり得るものである。なお、タイムスタンプはもちろん暗号化されていない。

【００５４】図３（ａ）に示すようなライセンス情報を用いる場合には、契約ユーザＤＢ１を検索する必要がない。すなわち、図８のステップＳ１１でライセンス情報生成の指示を受けたライセンス情報生成部８は、ステップＳ１５に進み、コンテンツキーＤＢ４からコンテンツＩＤ毎のコンテンツキーを検索し、また、シードＤＢ３から１９９７年１２月１日から１９９７年１２月３１日に有効なシードに対応したマスターキーを検索し（ステップＳ１６）、図３（ａ）に示すようなライセンス情報を生成し、コンテンツＩＤ以外の情報を暗号化する（ステップＳ１７）。

【００５５】なお、マスターキーシードは、ライセンス情報の暗号化に用いられたマスターキーに対応するものをライセンス情報の配信と同時にあるいは適宜配信されている。

【００５６】（３）再生装置

図９は、本実施形態に係る再生装置１０の構成例を示したもので、図１０は、再生装置１０のライセンス判定ユニット２０８の構成例を示したものである。

【００５７】以下、図１１、図１２に示すフローチャートを参照して再生装置１０およびライセンス判定ユニット２０８の各構成部およびこれらの動作について説明する。放送受信装置１００は、地上局２００からの放送波を受信し、放送配信されたライセンス情報とマスターキーシードが再生装置１０のフィルタ２０２に入力する（ステップＳ２１）。

【００５８】フィルタ２０２ではライセンス情報とマスターキーシードとを分別し、マスタキーシードであれば、それをライセンス判定ユニット２０８へ転送し、ライセンス情報であれば、それをライセンス情報蓄積部２０４へ転送する（ステップＳ２２～ステップＳ２５）。

【００５９】ライセンス判定ユニット２０８では、マスターキー生成部８０１にてマスターキーシードからマスターキーを生成して、マスターキー格納部８０２に格納する（ステップＳ２６）。マスターキーを生成する際には、予め契約管理装置との間で定められた同一のアルゴリズムを用いてマスターキーシードから共有鍵としてのマスターキーを生成するようにしてもよい。また、ライセンス判定ユニット２０８のマスターキー生成部８０１では、新たにマスターキーシードが入力される度にそれを用いてマスターキーを生成して、それをマスターキー格納部８０２に格納されている前回までのマスターキーに上書きして保持することにより、マスターキーが更新されてもその都度その更新された新たなマスターキーを得ることができる。

【００６０】ライセンス情報蓄積部２０４では、入力されたライセンス情報をコンテンツＩＤ別に保存する。すなわち、ライセンス情報が入力される度に、それに含まれるコンテンツＩＤをチェックし、既に同じコンテンツＩＤのライセンス情報が保存されている場合は、それに上書きしていく。ライセンス情報にタイムスタンプが含まれている場合は、それに示される日時をチェックして、所定期間経過したものは廃棄する、新たに入力されたライセンス情報で上書きしていく、等の制御が行える。

【００６１】さて、再生装置１０にＤＶＤディスクが挿入されると（ステップＳ３１）、ＤＶＤドライブ２０６は、まず、当該ディスクからコンテンツＩＤを読み出し、ライセンス情報選択部２０７へ転送する（ステップＳ３２）。ライセンス情報選択部２０７は、当該コンテンツＩＤを有するライセンス情報を、ライセンス情報蓄積部２０４から検索する（ステップＳ３３）。当該コンテンツＩＤを有するライセンス情報が存在するときは、それをライセンス判定ユニット２０８に転送する（ステップＳ３４～ステップＳ３５）。当該ライセンスＩＤを有するライセンス情報が見つからないとき、あるいは、あったとしてもタイムスタンプに示される時刻から無効なもの（期限きれ）と判断できるときは、その後の処理を中止する。

【００６２】ラインセンス判定ユニット２０８の復号部８０４では、マスターキー格納部８０２に格納されているマスターキーを用いてライセンス情報選択部２０７から転送されたライセンス情報を復号する（ステップＳ３６）。

【００６３】ここで、図３（ｂ）に示したようなライセンス情報の場合のライセンス判定ユニット２０８の判定部８０５における判定処理について説明する。この場合、判定部８０５では、復号されたライセンス情報に含まれていた端末ＩＤにＩＤ格納部８０３に予め格納されている自身の端末ＩＤが一致するか、あるいは含まれているかをチェックする。自身の端末ＩＤと一致あるいは自身の端末ＩＤが含まれていれば当該ライセンス情報は有効と判定し、復号されたライセンス情報に含まれていたコンテンツキーをデコーダ（例えば、ＭＰＥＧ２デコーダ）２０９へ転送する（ステップＳ３７～ステップＳ３８）。それ以外の場合は、当該ライセンス情報は無効と判定し、以後の処理は中止する。

【００６４】次に、図３（ａ）に示したようなライセンス情報の場合のライセンス判定ユニット２０８の判定部８０５における判定処理について説明する。この場合、判定部８０５では、特に判定処理はおこなわなくてもよく、そのまま、復号されたライセンス情報に含まれていたコンテンツキーをＭＰＥＧ２デコーダ２０９へ転送する（ステップＳ３７～ステップＳ３８）。この場合の顧客毎の視聴期間の管理は、例えば、従来からの衛星放送の受信契約管理の場合と同様、各放送受信装置１００に対し放送波受信可否を制御するための信号（ＯＮ／ＯＦＦ信号）を送ることにより行っているため、放送受信装置１００が一旦ＯＦＦ信号を受けたときはそれ以後ＯＮ信号を再び受信するまで放送波の受信動作を行うことはないからである。

【００６５】ＤＶＤドライブ２０６では、ＤＶＤディスクから暗号化されたコンテンツ情報を読み取って、それをＭＰＥＧ２デコーダ２０９へ転送する（ステップＳ３９）。

【００６６】ＭＰＥＧ２デコーダ２０９はライセンス判定ユニット２０８から転送されてきたコンテンツ情報を用いて該暗号化されたコンテンツ情報を復号し、さらにＤ／Ａ変換して所定の表示装置へ出力する（ステップＳ４０からステップＳ４１）。

【００６７】なお、ライセンス情報にタイムスタンプが含まれている場合、ライセンス判定ユニット２０８に時計が具備されているとき、判定部８０５では、タイムスタンプにて示されている日時と、この時計にて計時されている日時とを比較して、当該ライセンス情報の有効／無効を判定してもよい。また、ライセンス情報に含まれるタイムスタンプに示され時刻情報を用いて、当該時計の時間設定を行うようにしてもよい。これらの詳細処理動作は、特願平９－１２２５１１号に記載されている。

【００６８】

【発明の効果】以上説明したように、本発明の契約管理装置によれば、ＤＶＤ等の記録媒体に記録されたコンテンツ情報を再生する再生装置を視聴契約に基づき放送にて制御でき、ＤＶＤ等の記録媒体に記録されたディジタル化された著作物（コンテンツ情報）の視聴を契約期間に限って視聴可能にすることができる。

【００６９】また、本発明の再生装置によれば、放送配信されるライセンス情報に基づき、ＤＶＤ等の記録媒体に記録された暗号化されたコンテンツ情報の再生を当該コンテンツ情報の視聴契約期間に限って可能にすることがきる。

【図面の簡単な説明】

【図１】本発明の実施形態に係る情報流通サービスを提供するためのシステム構成例を示した図。

【図２】コンテンツ情報の記録された例えばＤＶＤ－ＲＯＭ等の記録媒体の記録データの構成例を示した図。

【図３】ライセンス情報のデータ構成例を示した図。

【図４】契約管理装置の構成例を示した図。

【図５】契約ユーザＤＢに記憶されるユーザ情報のデータ構成例を示した図。

【図６】シードＤＢに記憶される情報のデータ構成例を示した図。

【図７】コンテンツキーＤＢに記憶される情報のデータ構成例を示した図。

【図８】図４の契約管理装置の動作を説明するためのフローチャート。

【図９】再生装置の構成例を示した図。

【図１０】図９のライセンス判定ユニットの構成例を示した図。

【図１１】図９の再生装置および図１０のライセンス判定ユニットの動作を説明するためのフローチャート。

【図１２】図９の再生装置および図１０のライセンス判定ユニットの動作を説明するためのフローチャート。

【符号の説明】

放送管理装置

１…契約ユーザデータベース

３…シードデータベース

４…コンテンツキーデータベース

５…ライセンス情報データベース

８…ライセンス情報生成部

９…ライセンス情報生成制御部

１２…ライセンス情報出力要請部

１３…放送装置

１４…スケジューリング部

再生装置

２０２…フィルタ

２０４…ライセンス情報蓄積部

２０６…ＤＶＤドライブ

２０７…ライセンス情報選択部

２０８…ライセンス判定ユニット

２０９…ＭＰＥＧデコーダ

８０１…マスターキー生成部

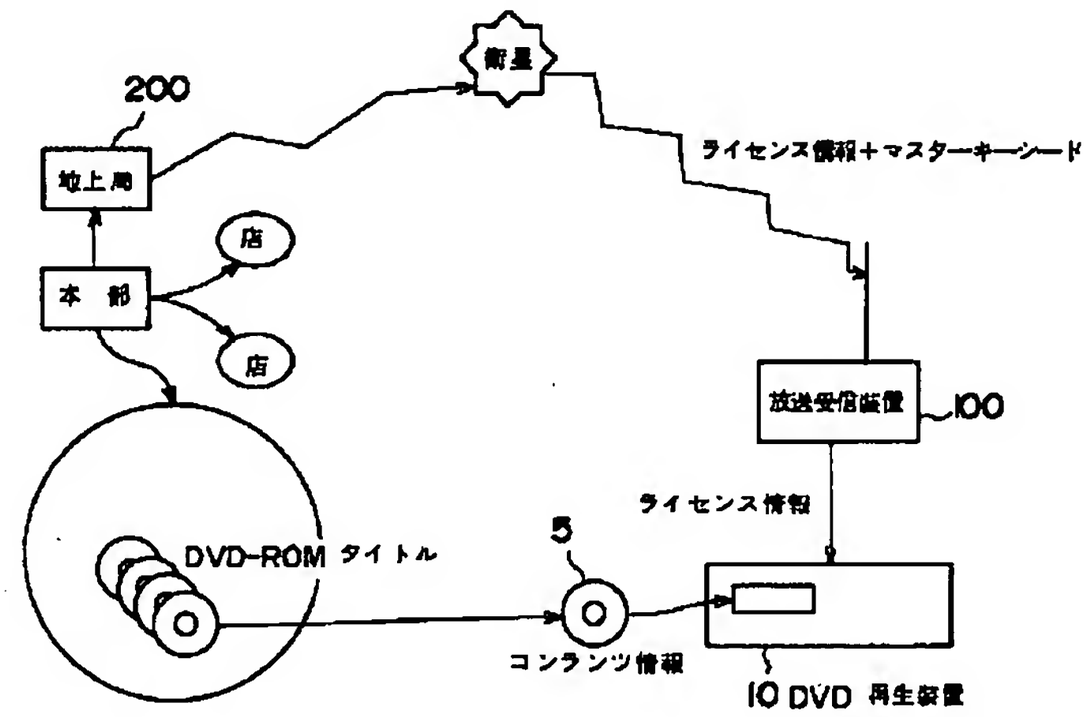
８０２…マスターキー格納部

８０３…ＩＤ格納部

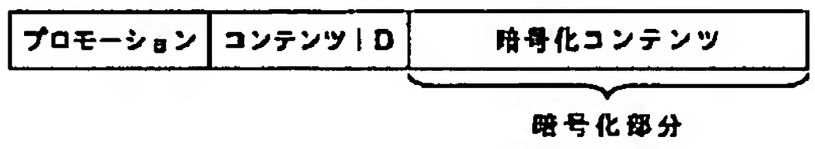
８０４…復号部

８０５…判定部

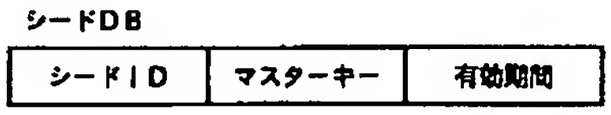
【図１】



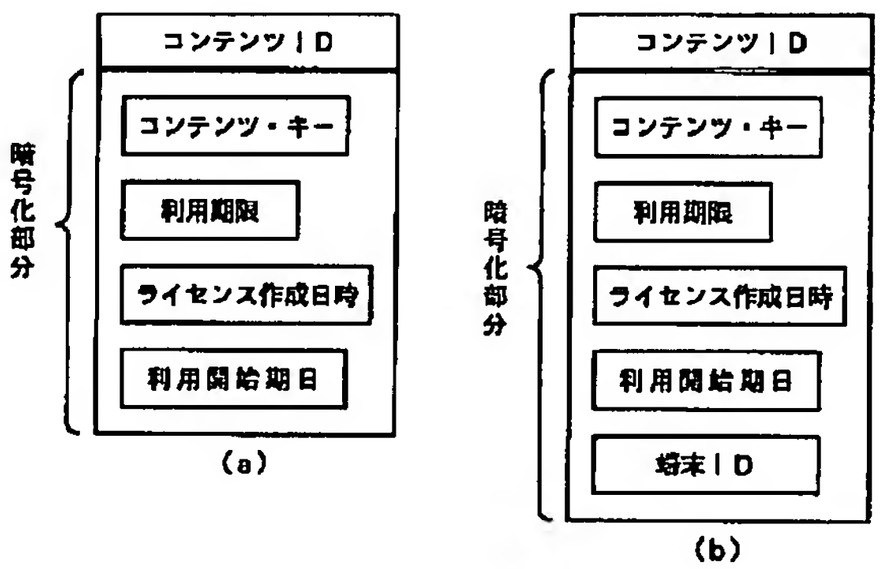
【図２】



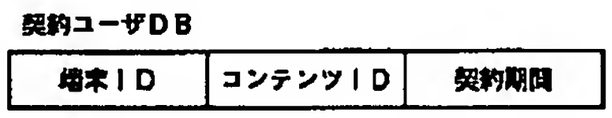
【図６】



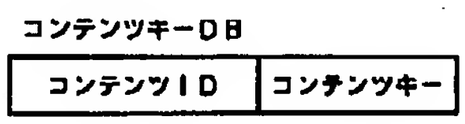
【図３】



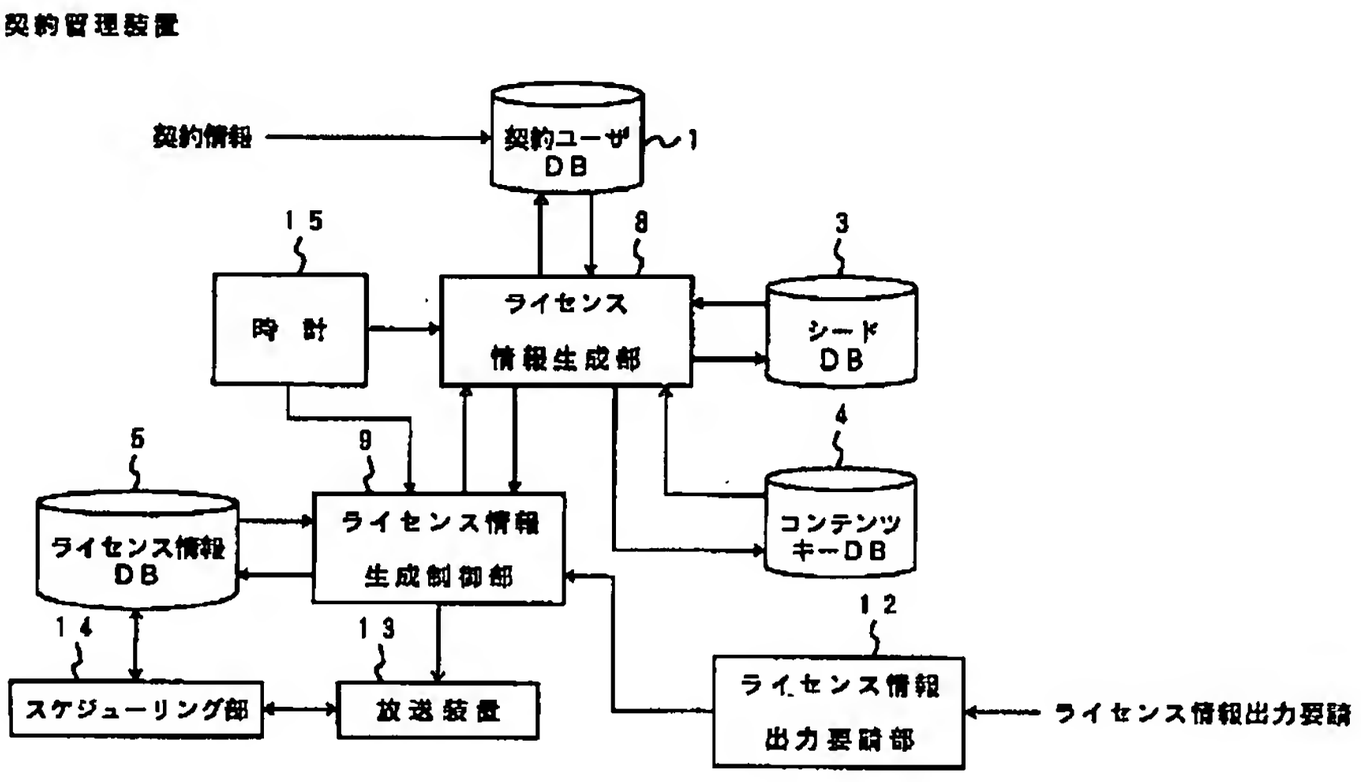
【図５】



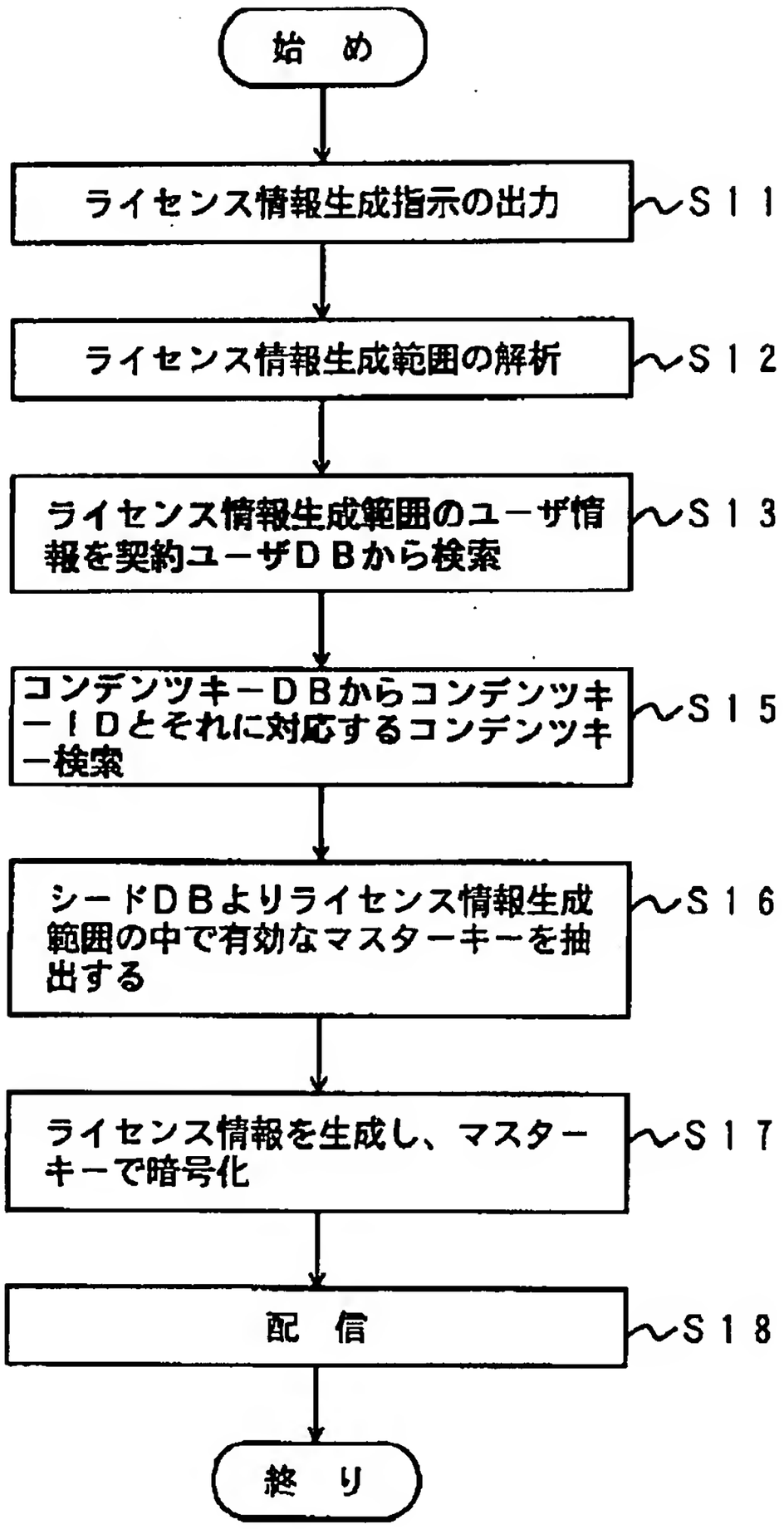
【図７】



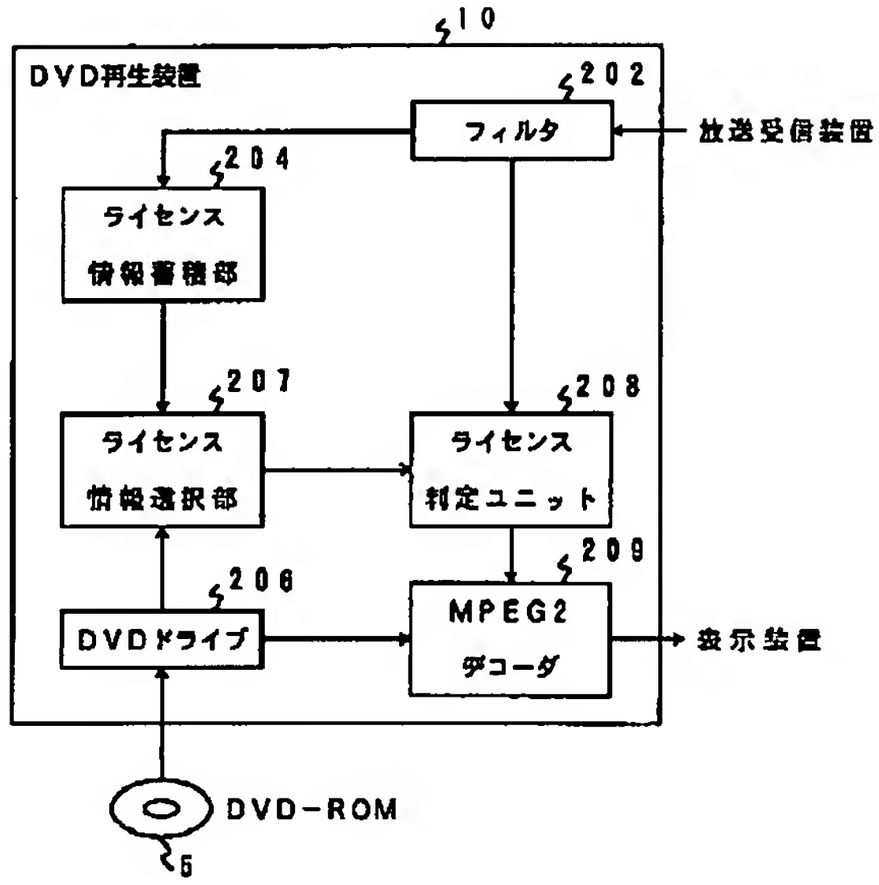
【図４】



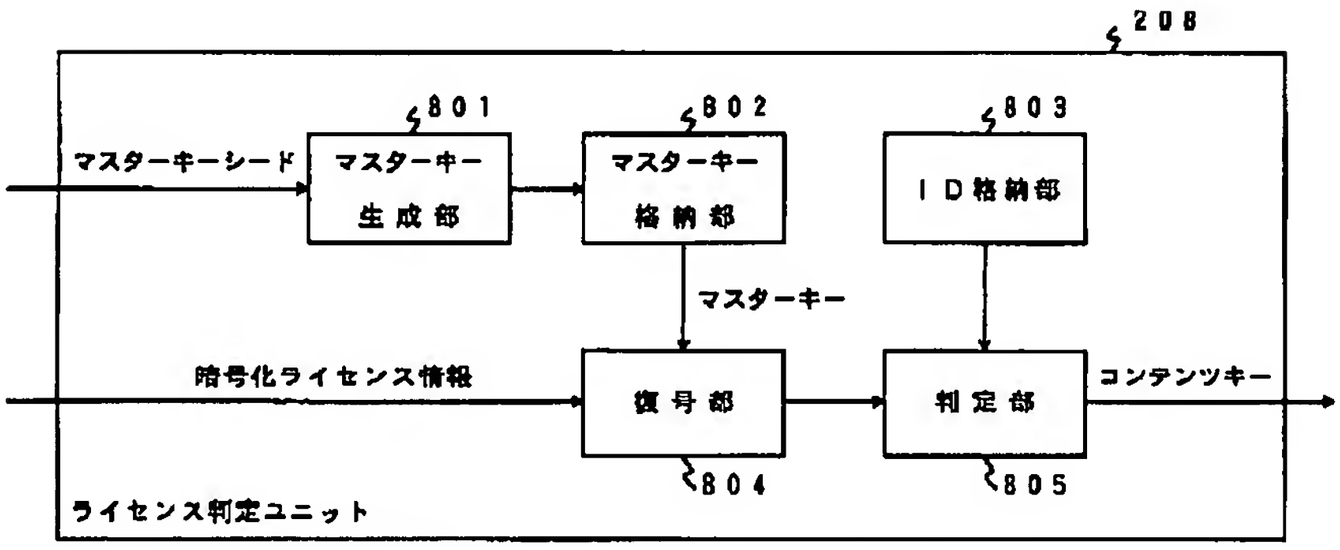
【図８】


始　め
ライセンス情報生成指示の出力
S１１
ライセンス情報生成範囲の解析
S１２
ライセンス情報生成範囲のユーザ情報を契約ユーザＤＢから検索
S１３
コンテンツキーＤＢからコンテンツキーＩＤとそれに対応するコンテンツキー検索
S１５
シードＤＢよりライセンス情報生成範囲の中で有効なマスターキーを抽出する
S１６
ライセンス情報を生成し、マスターキーで暗号化
S１７
配　信
S１８
終　り

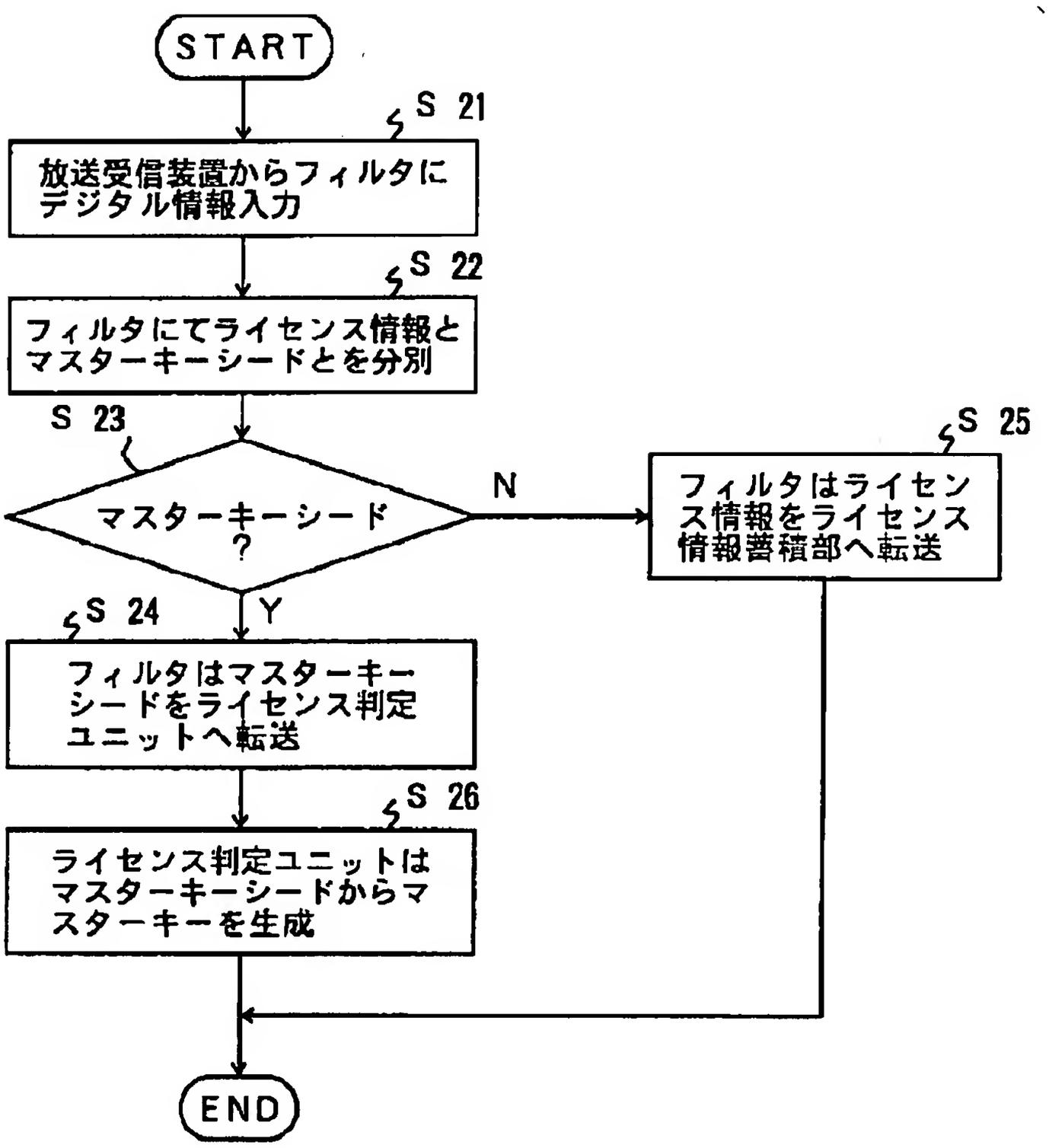
【図９】


１０
DVD再生装置
２０２
フィルタ
放送受信装置
２０４
ライセンス情報蓄積部
２０７
ライセンス情報選択部
２０８
ライセンス判定ユニット
２０９
MPEG2デコーダ
表示装置
２０６
DVDドライブ
DVD-ROM
５

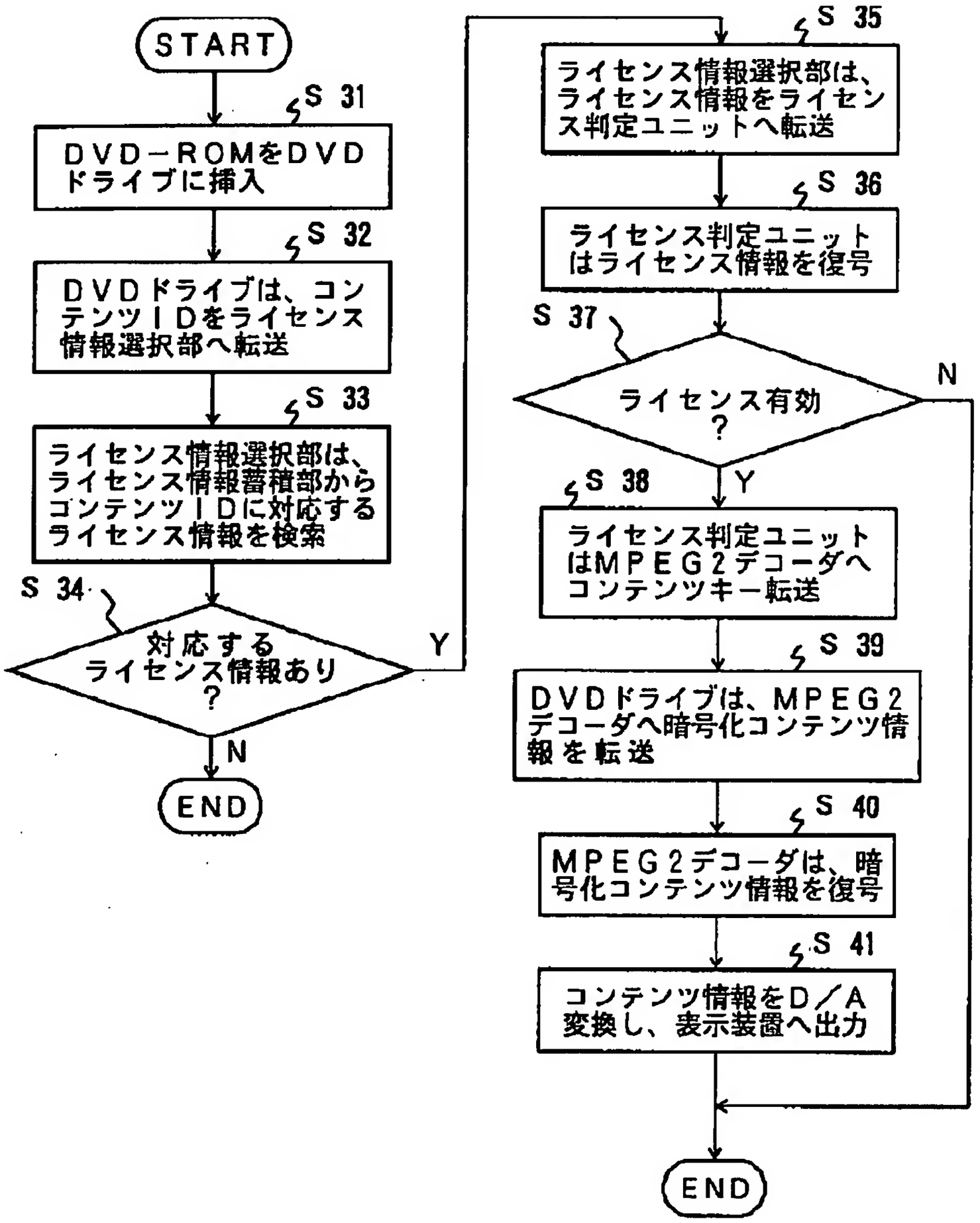
【図１０】


２０８
８０１
マスターキー生成部
８０２
マスターキー格納部
８０３
ＩＤ格納部
マスターキーシード
マスターキー
暗号化ライセンス情報
復号部
判定部
コンテンツキー
８０４
８０５
ライセンス判定ユニット

【図１１】


START
S 21
放送受信装置からフィルタにデジタル情報入力
S 22
フィルタにてライセンス情報とマスターキーシードとを分別
S 23
マスターキーシード？
N
S 25
フィルタはライセンス情報をライセンス情報蓄積部へ転送
Y
S 24
フィルタはマスターキーシードをライセンス判定ユニットへ転送
S 26
ライセンス判定ユニットはマスターキーシードからマスターキーを生成
END

【図１２】


START
S 31
DVD－ROMをDVDドライブに挿入
S 32
DVDドライブは、コンテンツＩＤをライセンス情報選択部へ転送
S 33
ライセンス情報選択部は、ライセンス情報蓄積部からコンテンツＩＤに対応するライセンス情報を検索
S 34
対応するライセンス情報あり？
Y
N
END
S 35
ライセンス情報選択部は、ライセンス情報をライセンス判定ユニットへ転送
S 36
ライセンス判定ユニットはライセンス情報を復号
S 37
ライセンス有効？
N
Y
S 38
ライセンス判定ユニットはMPEG2デコーダへコンテンツキー転送
S 39
DVDドライブは、MPEG2デコーダへ暗号化コンテンツ情報を転送
S 40
MPEG2デコーダは、暗号化コンテンツ情報を復号
S 41
コンテンツ情報をD／A変換し、表示装置へ出力
END

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-213553
(43)Date of publication of application : 06.08.1999
(51)Int.Cl. G11B 20/10
G09C 1/00
H04L 9/32
(21)Application number : 10-015788 (71)Applicant : TOSHIBA CORP
(22)Date of filing : 28.01.1998 (72)Inventor : KAMIBAYASHI TATSU
AKIYAMA KOICHIRO
TSUJIMOTO SHUICHI

(54) CONTRACT MANAGING DEVICE AND REPRODUCING DEVICE

(57)Abstract:
PROBLEM TO BE SOLVED: To make literary works audio-visual within the period of a contract by controlling the reproducing operation of a reproducing device with a signal transmitted to control the receiving operation of broadcasting waves based on an audio-visual contract.
SOLUTION: When a DVD-ROM is inserted into a DVD reproducing device and a reproduction is instructed, the device retrieves license information whose ID is matched with ciphered content information from a license storage part. When the license information corresponding to the ID of the content information exist, the efficiency of the license information is checked, and when the license information are not effective because the effective period of the information is expired or the like, the DVD reproducing device does not perform the decoding and the reproducing of the content information. On the other hand, when the information are effective, the device performs the decoding and the reproducing of the content information. Thus, a charge (a charge being an amount equivalent to a literary property) with respect to the viewing of the content information of a customer is replaced with the reception contract fee of a satellite broadcast in this manner.

LEGAL STATUS [Date of request for examination] 26.03.2001
[Date of sending the examiner's decision of rejection] 02.12.2003
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection] 2004-000220
[Date of requesting appeal against examiner's decision of rejection] 05.01.2004
[Date of extinction of right]

CLAIMS

[Claim(s)]
[Claim 1] It is contract-management equipment for controlling the regenerative apparatus which reproduces the enciphered contents information which was recorded on the record medium by broadcast based on a viewing-and-listening contract. The enciphered control information including the 1st key information which decodes this contents information that was matched with each of each contents information, and that was enciphered at least, Contract-management equipment characterized by controlling playback actuation of said regenerative apparatus by the signal distributed in order to provide the means which carries out broadcast distribution of the key creation information required in order to generate the 2nd key information which decodes the enciphered this control information and to control reception actuation of a broadcast wave based on a viewing-and-listening contract.
[Claim 2] It is contract-management equipment for controlling the regenerative apparatus which reproduces the enciphered contents information which was recorded on the record medium by broadcast based on a viewing-and-listening contract. The enciphered control information containing the 1st key information which decodes this contents information that was matched with each of each contents information, and that was enciphered at least, and the identification information of said regenerative apparatus, The means which carries out broadcast distribution of the key creation information required in order to generate the 2nd key information which decodes said enciphered control information is provided. Contract-management equipment characterized by permitting playback of the contents information based on this control information only to the regenerative apparatus specified in the identification information contained in said control information.
[Claim 3] Said key creation information is contract-management equipment according to claim 1 or 2 characterized by being updated for every predetermined period.
[Claim 4] The enciphered control information including the 1st key information which decodes this contents information by which broadcast distribution was carried out, that was matched with each of each contents information, and that was enciphered at least, It is based on key creation information required in order to generate the 2nd key information which decodes the enciphered this control information. A decode means to be the regenerative apparatus which reproduces the enciphered contents information which was recorded on the record medium, and to decode said enciphered control information using the 2nd key information generated based on said key creation information, The playback means which carries out decode playback of the enciphered contents information which was recorded on said record medium using the 1st key information contained in the control information decoded with this decode means, It is contract-management equipment which possesses and is characterized by controlling said playback means by the signal distributed in order to control reception actuation of a broadcast wave based on a viewing-and-listening contract.
[Claim 5] The enciphered control information containing the 1st key information which decodes this contents information by which broadcast distribution was carried out, that was matched with each of each contents information, and that was enciphered at least, and the identification information of said regenerative apparatus, It is based on key creation information required in order to generate the 2nd key information which decodes said enciphered control information. A decode means to be the regenerative

apparatus which reproduces the enciphered contents information which was recorded on the record medium, and to decode said enciphered control information using the 2nd key information generated based on said key creation information, The playback means which carries out decode playback of the enciphered contents information which was recorded on said record medium using the 1st key information contained in the control information decoded with this decode means, It is contract-management equipment which possesses and is characterized by said playback means judging the propriety of playback of said contents information by said identification information contained in said control information.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention distributes the control information which distributes at a customer contents information enciphered with record media, such as DVD, (charge), for example, includes the decode key information on contents information in satellite broadcasting service to a regenerative apparatus, and relates to the distribution system of information whose viewing and listening is enabled according to the viewing-and-listening contract (for example, viewing-and-listening period) of the contents information.

[0002]

[Description of the Prior Art] In recent years, development of the advanced information record medium which realizes the large capacity of development of communication technology, such as a digital-information-processing technique and broadband ISDN, DVD, etc., high definition, and quality of loud sound is progressing. The digitized work is distributed to a user in large quantities through a network, a record medium, etc., and the environment where a user can use them freely is being born as diversification of such an informational means of communication and an advancement progress. Such an environment increases the opportunity for the unapproved duplicate of a work, an unapproved alteration, the circulation that an author does not mean to take place, and makes concern whether self profits are unfairly injured for the rightful claimant of a work hold.

[0003] While circulating the work digitized quickly and easily so that concern of the rightful claimant of such a work can be wiped and paid, development of the system on condition of protection of the copyright which can offer the use environment of digital information where they can be used proper serves as an important future technical problem.

[0004] While DVDs are mass personal computer media replaced with CD-ROM, in order to be able to expect the breadth to various applications, such as a movie, music, a game, and karaoke, and to aim at the spread of such DVDs, the title price of DVD is held down low or the expansion to a rental DVD commercial scene is also expected. Therefore, the circulation system of the information on condition of the protection of the copyright over information based on the idea of charging to digitized not possession but the use of a work which was recorded on record media, such as DVD, becomes indispensable also from such a viewpoint.

[0005] On the other hand, much more substantial service is expected and it is thought that the leading role of future broadcast service is played as digital broadcast starts in a

communication satellite (CS) and digitization progresses to a cable TV and ground broadcast.
[0006] The greatest description of digital broadcast is that could aim at improvement in the utilization ratio of the frequency which transmission of a program takes, and the steep increment in the number of broadcast channels was attained by installation of an information-compression technique as compared with analog broadcasting. Furthermore, for a ** reason, offer of quality and homogeneous service of an advanced error correction technique is attained by application.
[0007] By digitization of broadcast, offer of the multimedia service by various information gestalten (an image, voice, an alphabetic character, data, etc.) is attained, and the system for offering such service is also appearing one after another.
[0008] In case the charged broadcast service which solves or decodes a scramble by such system based on the contents of a contract is offered, customer management adapted to a contract term must be able to be performed. The customer management adapted to a contract term enables viewing and listening of the program of a contract channel [within the contract term a contract of was made by payment of a predetermined tariff].
[0009] Moreover, it is necessary to provide only a just viewer with the key information for solving a scramble or a code with a receiving set certainly moreover (based on a contract channel and a contract term) also from from [when preventing unjust viewing and listening].
[0010]
[Problem(s) to be Solved by the Invention] Then, this invention aims at offering the distribution system of information which offers the use environment of the digital information on condition of protection of the copyright based on the contract of viewing and listening of the digitized work while it circulates the digitized work quickly and easily.
[0011] This invention is contract-management equipment for controlling the regenerative apparatus which reproduces the enciphered contents information which was recorded on the record medium by broadcast based on a viewing-and-listening contract. The regenerative apparatus which reproduces the contents information recorded on record media, such as DVD, is controllable by broadcast based on a viewing-and-listening contract. It aims at offering the contract-management equipment which can enable viewing and listening of viewing and listening of the digitized work (contents information) which was recorded on record media, such as DVD, only within a contract term.
[0012] Moreover, this invention aims at offering the regenerative apparatus which enabling playback of the enciphered contents information which was recorded on record media, such as DVD, only within the viewing-and-listening contract term of the contents information concerned based on the control information by which broadcast distribution is carried out cuts.
[0013]
[Means for Solving the Problem] The contract-management equipment of this invention is contract-management equipment for controlling the regenerative apparatus which reproduces the enciphered contents information which was recorded on the record medium by broadcast based on a viewing-and-listening contract. The enciphered control information including the 1st key information which decodes this contents information that was matched with each of each contents information, and that was

enciphered at least, The means which carries out broadcast distribution of the key creation information required in order to generate the 2nd key information which decodes the enciphered this control information is provided. By controlling playback actuation of said regenerative apparatus by the signal distributed in order to control reception actuation of a broadcast wave based on a viewing-and-listening contract The regenerative apparatus which reproduces the contents information recorded on record media, such as DVD, can be controlled by broadcast based on a viewing-and-listening contract, and viewing and listening of viewing and listening of the digitized work (contents information) which was recorded on record media, such as DVD, can be enabled only within a contract term.

[0014] Moreover, the contract-management equipment of this invention is contract-management equipment for controlling the regenerative apparatus which reproduces the enciphered contents information which was recorded on the record medium by broadcast based on a viewing-and-listening contract. The enciphered control information containing the 1st key information which decodes this contents information that was matched with each of each contents information, and that was enciphered at least, and the identification information of said regenerative apparatus, The means which carries out broadcast distribution of the key creation information required in order to generate the 2nd key information which decodes said enciphered control information is provided. By permitting playback of the contents information based on this control information only to the regenerative apparatus specified in the identification information contained in said control information The regenerative apparatus which reproduces the contents information recorded on record media, such as DVD, can be controlled by broadcast based on a viewing-and-listening contract, and viewing and listening of viewing and listening of the digitized work (contents information) which was recorded on record media, such as DVD, can be enabled only within a contract term.

[0015] The enciphered control information including the 1st key information which decodes this contents information that was matched with each of each contents information, and that was enciphered at least that broadcast distribution of the regenerative apparatus of this invention was carried out, It is based on key creation information required in order to generate the 2nd key information which decodes the enciphered this control information. A decode means to be the regenerative apparatus which reproduces the enciphered contents information which was recorded on the record medium, and to decode said enciphered control information using the 2nd key information generated based on said key creation information, The playback means which carries out decode playback of the enciphered contents information which was recorded on said record medium using the 1st key information contained in the control information decoded with this decode means, By being controlled by the signal distributed in order that it may provide and said playback means may control reception actuation of a broadcast wave based on a viewing-and-listening contract enabling playback of the enciphered contents information which was recorded on record media, such as DVD, only within the viewing-and-listening contract term of the contents information concerned based on the license information by which broadcast distribution is carried out cuts.

[0016] Moreover, the enciphered control information containing the 1st key information which decodes this contents information that was matched with each of each contents

information, and that was enciphered at least that broadcast distribution of the regenerative apparatus of this invention was carried out, and the identification information of said regenerative apparatus, It is based on key creation information required in order to generate the 2nd key information which decodes said enciphered control information. A decode means to be the regenerative apparatus which reproduces the enciphered contents information which was recorded on the record medium, and to decode said enciphered control information using the 2nd key information generated based on said key creation information, The playback means which carries out decode playback of the enciphered contents information which was recorded on said record medium using the 1st key information contained in the control information decoded with this decode means, When it provides and said playback means judges the propriety of playback of said contents information by said identification information contained in said control information enabling playback of the enciphered contents information which was recorded on record media, such as DVD, only within the viewing-and-listening contract term of the contents information concerned based on the license information by which broadcast distribution is carried out cuts.

[0017]

[Embodiment of the Invention] Hereafter, the operation gestalt of this invention is explained with reference to a drawing.

(1) The schematic diagram 1 of distribution-of-information service shows the example of a system configuration for offering the distribution-of-information service concerning the operation gestalt of this invention. It is enciphered, for example, the contents information as digitized works (for example, movie etc.) is recorded on the record media (taking the case of the case of DVD-ROM, it explains hereafter) 5, such as DVD-ROM, for example, is distributed through a rental operating company.

[0018] A rental operating company's headquarters distributes DVD-ROM with which the contents information as which it was enciphered for every title was recorded on sequence each store. A customer cannot view and listen to this contents information only by purchasing DVD-ROM with which the contents information on a desired title was recorded. The key information (henceforth, contents key) for decoding the enciphered contents information which was recorded on DVD-ROM, and reproducing is required. This contents key is distributed to the receiving set 100 which each customer has in satellite broadcasting service from Satellite Broadcasters 200 which was enciphered, for example, has tied up with the headquarters of a rental firm.

[0019] When a customer purchases DVD-ROM of this contents information at a sequence store, he pays the tariff according to the viewing-and-listening contract which defined the viewing-and-listening period at least. It is just going to consider as the purpose of this invention that a customer enables it to view and listen to the contents information recorded on the DVD-ROM concerned with the regenerative apparatus 10 of DVD-ROM which a customer has based on this viewing-and-listening contract.

[0020] In addition, specifically, the contents key which decodes the enciphered contents information which was recorded on DVD-ROM is contained in the license information (after-mentioned) which is distributed in satellite broadcasting service and which was enciphered in part (the following explanation).

[0021] License information is generated by the contract-management equipment which is installed in the case of this operation gestalt (for example, the headquarters of a rental firm). The license information distributed in the satellite broadcasting service received with the receiving set 100 (it is desirable that it is the existing thing) inputs into the regenerative apparatus 10 which a customer has. For example, decode the encryption part of this license information by the master key generated based on the master key seed separately distributed in satellite broadcasting service, and predetermined judgment processing (it mentions later for details) is performed. When it judges that viewing and listening of this contents information in the scope of the viewing-and-listening contract which the customer concerned performed is possible, the enciphered contents information which was recorded on DVD-ROM using the contents key contained in the license information concerned is decoded, and it reproduces. On the contrary, if license information effective in a regenerative apparatus 10 is not inputted, the enciphered contents information which was recorded on DVD-ROM cannot be decoded.

[0022] The license information distributed in satellite broadcasting service is received by each broadcast receiving set 100. That is, the customer who is going to use distribution-of-information service of this invention has to make the reception contract of the satellite broadcasting service concerned beforehand like the case where reception service of a certain satellite broadcasting service is received from the former. Otherwise, license information is correctly unacquirable with the broadcast receiving set 100.

[0023] The license information received with the broadcast receiving set 100 is sent to a regenerative apparatus 10. A regenerative apparatus 10 saves the inputted license information in the license information storage section inside a regenerative-apparatus opportunity.

[0024] License information may be repeatedly broadcast according to the suitable schedule. About this schedule method, it mentions later. The expiration date information on the license information concerned may be included in license information.

[0025] Next, the outline of the distribution-of-information service concerning this invention is explained. The customer who is going to use the distribution-of-information service concerning this invention shall purchase the DVD regenerative apparatus 10 which is adapted for this service, and shall acquire DVD-ROM with which the contents information on a desired title was further recorded from the sequence store of the operating company who offers this distribution-of-information service.

[0026] As shown in drawing 2 , the enciphered contents information is recorded on DVD-ROM. Even if it purchases DVD-ROM with which the contents information on a desired title was recorded, since this contents information is enciphered, if it remains as it is, it cannot view and listen. Therefore, in case DVD-ROM with which this contents information was recorded is purchased, there is no need of not necessarily paying the tariff of a copyright considerable amount. That is, the customer who is going to use the distribution-of-information service concerning this invention becomes possible [the thing of for example, "price / of the DVD-ROM itself / + commission" extent for which DVD-ROM is extremely acquired by the low price].

[0027] If a customer inserts the purchased DVD-ROM concerned in the DVD regenerative apparatus 10 and playback is directed, he will retrieve the license information which is in agreement with ID from the license information storage section of

the DVD regenerative apparatus 10 to the contents information concerned. If the license information on early does not exist, playback of contents information is not performed from the DVD-ROM concerned. When the license information corresponding to the content ID concerned exists, the DVD regenerative apparatus 10 checks the effectiveness of license information. When license information is not effective, the DVD regenerative apparatus 10 does not perform decode playback of the contents information concerned -- the expiration date has passed. On the other hand, if license information is effective, as for the DVD regenerative apparatus 10, decode of the contents information concerned and playback will be performed.

[0028] Thus, accounting (namely, tariff of a copyright considerable amount) to viewing and listening of a customer's contents information is replaced by the charge of a reception contract of satellite broadcasting service. The customer who is going to use distribution-of-information service pays the subscription fee of the fixed amount of money for a broadcast reception contract an epilogue, for example, every month, first. Next, a subscriber chooses the contents information on the title of liking at a rental operating company's sequence store. What is necessary is just to pay the amount of money of "price [of the record medium itself] + commission" extent to acquisition of the record medium with which encryption contents were recorded, as already stated. Then, a customer can reproduce the contents information brought home freely according to a reception contract with the DVD regenerative apparatus 10. It is because the newest effective license information is supplied to the DVD regenerative apparatus 10 from the broadcast receiving set 100.

[0029] For example, the license information (for example, thing corresponding to contents ** of content ID "#21243") distributed by 23:59 on July 7 presupposes that it has the expiration date called 23:59 on July 14 by broadcast distribution of license information. What has the expiration date called 23:59 on July 21 for the license information corresponding to the contents information on content ID "#21243" will be broadcast by 23:59 on July 14 after 0:00 on July 8, and will be stored in the DVD regenerative apparatus 10. Thereby, a customer can reproduce the contents information on content ID "#21243" at any time.

[0030] Now, when the subscriber of the broadcast concerned cancels a reception contract as of July 22, a rental operating company will be notified of the purport of rescission by July 14. the receiving set 100 of ****** and the customer concerned -- 23:59 on July 14 -- with -- **** -- reception of license broadcast is stopped. In this case, the license information on ID "#21243" which has expiration date 7 month 28 day 23 o'clock 59 broadcast after 0:00 on July 15 is not distributed to the receiving set 100 concerned, and is not accumulated in the DVD regenerative apparatus 10 of the customer concerned.

[0031] It becomes impossible therefore, for the customer concerned to view and listen to the contents information on ID "#21243" after 23:59 on July 21. The system which offers hereafter the distribution-of-information service which relates to this invention more concretely is explained.

[0032] As shown in drawing 2 , the contents information enciphered by the contents key, the identification information (content ID) of this contents information, and the information for promotions that the contents of this contents information are introduced are recorded on DVD-ROM. It is not enciphered as the information for content ID and

promotions. In addition, contents keys differ for every contents information. Moreover, one content ID shall be given at a time for every title. Furthermore, a contents key is beforehand defined for every title.
[0033] Drawing 3 is what showed the example for the data format of license information, the (a) Fig. is license information in case identification information (terminal ID) for identifying each of the regenerative apparatus which the customer by whom the reception contract was made by license information has is not included, and the (b) Fig. shows the license information in the case of including the terminal ID for limiting the regenerative apparatus which receives the license information concerned.
[0034] The license information shown in drawing 3 (a) is generated one [at a time] for every title of contents information, and the content ID of the title concerned and a contents key are contained at least. Content ID is not enciphered but the other information (at least contents key) is enciphered with the master key.
[0035] When using license information as shown in drawing 3 (a), management of the viewing-and-listening period for every customer may be performed by sending the signal (ON/OFF signal) for controlling broadcast wave no ready for receiving to each broadcast receiving set 100 like the case of the receiving contract management of the satellite broadcasting service from the former. That is, broadcast distribution of the ON signal is carried out to the broadcast receiving set 100 of the customer concerned at the time of initiation of a customer's viewing-and-listening period, and broadcast distribution of the OFF signal is carried out to the broadcast receiving set 100 of the customer concerned at the time of termination of a viewing-and-listening period, for example. Reception of a broadcast wave is started by receiving ON signal with which the broadcast receiving set 100 was distributed to the broadcast receiving set concerned, and control which makes reception of a broadcast wave improper by receiving an OFF signal is performed.
[0036] As for the license information shown in drawing 3 (b), the content ID of the title concerned, the contents key, and the terminal ID that specifies the regenerative apparatus with which the license information concerned is received are included at least. Content ID is not enciphered but the other information (at least a contents key, a terminal (ID)) is enciphered with the master key.
[0037] in addition, the terminal ID of the regenerative apparatus of each [information / which is shown in drawing 3 (b) / license] as a terminal ID only -- one -- indicating -- every customer -- the license information concerned -- generation -- you may distribute -- for example, the terminal ID -- lower -- several figures are indicated as a terminal ID and you may enable it to receive two or more regenerative apparatus at a time It cannot be overemphasized that latter one has the good distribution effectiveness of license information.
[0038] When using the license information shown in drawing 3 (b), management of the viewing-and-listening period for every customer can be performed by not indicating the terminal ID of a customer's regenerative apparatus 10 with which the contract term went out to the terminal ID of license information. In this case, it will be confirmed whether each of a regenerative apparatus 10 compares with the own terminal ID the terminal ID included in license information, and incorporates license information. during a contract term -- that of own terminal ID ** -- although -- although it was indicated or license information including the own terminal ID is distributed frequently, the own terminal ID is

no longer indicated by license information from the time of a contract term going out. Therefore, a regenerative apparatus 10 can perform decode of the enciphered contents information which was recorded harder [which cannot acquire effective license information] by DVD-ROM, and playback.
[0039] It is desirable to use a cipher system with the following descriptions for encryption of license information.
1) Put data, such as content ID and a contents key, in order in suitable sequence. Here, each data may be called the field.
[0040] 2) Disturb the sequence of the bit string of 1 according to a suitable algorithm. Under the present circumstances, it is desirable to perform a pit disturbance in the large range.
3) Encipher the data of 2 with a suitable key and a suitable cipher system. Not enciphering 1) as it is is based on the following reason. That is, the usual cipher system repeats the thing as which it was determined beforehand and to encipher for every suitable bit length. Therefore, it is possible by disturbing 2 to reduce the danger that each field of license information will be separated and changed.
[0041] (2) Contract-management equipment drawing 4 is what showed the example of a configuration of the contract-management equipment concerning this operation gestalt, is installed in the earth station 200 of drawing 1 , and is used.
[0042] An earth station 200 carries out broadcast distribution of license information and master key seed as showed drawing 3 (a) or drawing 3 (b). Parts other than content ID are enciphered with the master key among license information. As for a master key, updating for every fixed period is desirable because of improvement in the confidentiality of license information. Therefore, broadcast distribution of information required in order for a regenerative apparatus 10 to generate a master key, i.e., the master key seed, is carried out (at the time of periodical or renewal of a master key).
[0043] Now, the contract-management equipment of drawing 4 is for performing generation of license information, and encryption and carrying out broadcast distribution. If a broadcast reception contract is made among customers, the contents of a contract (content ID, viewing-and-listening period, etc.) will be registered into the contract user database (DB) 1.
[0044] Data are stored by the contract user DB1 in the format shown in drawing 5 . drawing 5 -- it is, and ID is the terminal ID of the regenerative apparatus 10 which a customer has, and is memorized in the end of receiving end in the format that the content ID by which this terminal ID was made to correspond and the viewing-and-listening contract was made, and a viewing-and-listening period were defined beforehand.
[0045] The seed database (DB) 3 is stored in the format which shows the master key generated from the master key seed for master key generation in drawing 6 with the seed ID and an expiration date. The master key seed corresponding to Seed ID may also be stored in seed DB3.
[0046] The contents key database (DB) 4 is stored in the format which the contents key for every title is made to correspond to content ID, and is shown in drawing 7 . Next, license information as shown in drawing 3 (b) is generated, and the procedure of sending this to a receiving set using broadcast equipment 13 is explained with reference to the flow chart shown in drawing 8 .

[0047] The license information generation control section 9 sends directions of license information generation to the license information generation section 8 (step S11). "send [the license information of the contract user who has contracted for one month after December 1, 1997]" These directions could be expressed by the bit string of the format which is the thing of the becoming contents and was defined beforehand. If such directions are issued, User Information (refer to drawing 5) a contract of is made for at least one month after December 1, 1997 from the contract user DB1 will be searched with the license information generation section 8, and the information concerned will be read (step S12 - step S13).
[0048] Here, the smallest unit of a contract term is one month, and a contract expiration date will start on the 1st, presupposes that it ends at the end of the month, and also makes a master key peculiar to this contract minimum period. That is, the master key in November shall not be changed within each moon using a different thing from it in December.
[0049] Next, the additional information generation section 8 searches the contents key for every content ID from the contents key DB4 (step S15), and searches the master key corresponding to the effective seed on December 31, 1997 from December 1, 1997 from seed DB3 (step S16).
[0050] Based on the information (the contents key corresponding to content ID and this content ID, each user's contents of a contract) acquired by the above, in the additional information generation section 8, license information as shown in drawing 3 (b) is generated, and information other than content ID is enciphered (step S17). The license information generated here is sent to the additional information generation control section 9 and broadcast equipment 13 one by one.
[0051] Broadcast equipment 13 changes license information into the broadcast wave of a predetermined frequency band, and carries out broadcast distribution towards a receiving set (step S18). In case the license information stored in the license information DB5 is distributed, or in case the scheduling section 14 distributes master key seed, it performs distribution control so that license information and master key seed may be certainly received by the receiving set by the side of each user.
[0052] That is, for example, in case the time of contract cancellation and the license information over the content ID of a popular title are transmitted after a reception contract at the time of contract modification, it is necessary to send the license information concerned frequently, and the scheduling section 14 performs distribution control of license information according to the distribution scheduling of the license information for it.
[0053] The time stump in which distribution time is shown may be contained in the license information generated in the license information generation section 8. As long as it can do, it is exact, and the time which a time stump shows can serve as time of day used as the criteria which were clocked by the clock 15 and which are used for various judgment processings from a regenerative apparatus 10. In addition, of course, the time stump is not enciphered.
[0054] When using license information as shown in drawing 3 (a), it is not necessary to search the contract user DB1. Namely, the license information generation section 8 which received directions of license information generation at step S11 of drawing 8 Progress to step S15 and the contents key for every content ID is searched from the

contents key DB4. Moreover, the master key corresponding to the effective seed on December 31, 1997 is searched from December 1, 1997 from seed DB3 (step S16), license information as shown in drawing 3 (a) is generated, and information other than content ID is enciphered (step S17).
[0055] In addition, the thing corresponding to the master key used for encryption of license information is distributed to master key seed being simultaneous or suitably as distribution of license information.
[0056] (3) Regenerative-apparatus drawing 9 is what showed the example of a configuration of the regenerative apparatus 10 concerning this operation gestalt, and drawing 10 shows the example of a configuration of the license judging unit 208 of a regenerative apparatus 10.
[0057] Hereafter, with reference to the flow chart shown in drawing 11 and drawing 12 , each configuration sections of a regenerative apparatus 10 and the license judging unit 208 and these actuation are explained. The broadcast receiving set 100 receives the broadcast wave from an earth station 200, and the license information by which broadcast distribution was carried out, and master key seed input it into the filter 202 of a regenerative apparatus 10 (step S21).
[0058] With a filter 202, license information and master key seed are classified, if it is master key seed, it will be transmitted to the license judging unit 208, and if it is license information, it will be transmitted to the license information storage section 204 (step S22 - step S25).
[0059] In the license judging unit 208, a master key is generated from master key seed in the master key generation section 801, and it stores in the master key storing section 802 (step S26). In case a master key is generated, you may make it generate the master key as a share key from master key seed using the same algorithm beforehand defined between contract-management equipment. Moreover, in the master key generation section 801 of the license judging unit 208, by using it, whenever master key seed is newly inputted, generating a master key, overwriting the master key to the last time in which it is stored by the master key storing section 802, and holding, even if a master key is updated, the updated new master key can be obtained each time.
[0060] In the license information storage section 204, the inputted license information is saved according to content ID. That is, it is overwritten, when the content ID contained in it whenever license information is inputted is checked and the license information on the same content ID is already saved. When the time stump is contained in license information, the time shown in it is checked and what carried out predetermined period progress can control ** overwritten for the newly inputted license information to discard.
[0061] Now, if a DVD disk is inserted in a regenerative apparatus 10 (step S31), first, the DVD drive 206 will read content ID from the disk concerned, and will transmit it to the license information selection section 207 (step S32). The license information selection section 207 retrieves the license information which has the content ID concerned from the license information storage section 204 (step S33). When the license information which has the content ID concerned exists, it is transmitted to the license judging unit 208 (step S34 - step S35). Subsequent processing is stopped, when the license information which has the license ID concerned is not found, or when [even if it is,] it can be judged as an invalid thing (term ****) from the time of day shown in a time stump.

[0062] In the decode section 804 of the Rhine sense judging unit 208, the license information transmitted from the license information selection section 207 using the master key stored in the master key storing section 802 is decoded (step S36).
[0063] Here, the judgment processing in the judgment section 805 of the license judging unit 208 in the case of license information as shown in drawing 3 (b) is explained. In this case, in the judgment section 805, it is confirmed whether the terminal ID of the self beforehand stored in the terminal ID included in the decoded license information at ID storing section 803 is in agreement, or it is contained. If the terminal ID of the own terminal ID, coincidence, or self is included, the contents key which judged with the license information concerned being effective, and was contained in the decoded license information will be transmitted to a decoder (for example, MPEG 2 decoder) 209 (step S37 - step S38). When other, it judges with the license information concerned being invalid, and future processings are stopped.
[0064] Next, the judgment processing in the judgment section 805 of the license judging unit 208 in the case of license information as shown in drawing 3 (a) is explained. In this case, it is not necessary to perform especially judgment processing, and the contents key contained in the decoded license information as it was is transmitted to the MPEG 2 decoder 209 in the judgment section 805 (step S37 - step S38). It is because management of the viewing-and-listening period for every customer in this case is performed by sending the signal (ON/OFF signal) for controlling broadcast wave no ready for receiving to each broadcast receiving set 100 like the case of the receiving contract management of the satellite broadcasting service from the former, so reception actuation of a broadcast wave is not performed until it receives ON signal again after it when the broadcast receiving set 100 once receives an OFF signal.
[0065] In the DVD drive 206, the contents information enciphered from the DVD disk is read, and it is transmitted to the MPEG 2 decoder 209 (step S39).
[0066] The MPEG 2 decoder 209 decodes the contents information this enciphered using the contents information transmitted from the license judging unit 208, it carries out D/A conversion further, and it is outputted to a predetermined display (from step S40 to step S41).
[0067] In addition, when the time stump is contained in license information and the clock possesses to the license judging unit 208, in the judgment section 805, the time shown with the time stump is compared with the time clocked by this clock, and effective/invalid of the license information concerned may be judged. Moreover, it is shown in the time stump contained in license information, and may be made to perform time setting of the clock concerned using time information. These detail processing actuation is indicated by Japanese Patent Application No. No. 122511 [nine to].
[0068]
[Effect of the Invention] As explained above, according to the contract-management equipment of this invention, the regenerative apparatus which reproduces the contents information recorded on record media, such as DVD, can be controlled by broadcast based on a viewing-and-listening contract, and viewing and listening of viewing and listening of the digitized work (contents information) which was recorded on record media, such as DVD, can be enabled only within a contract term.
[0069] moreover, according to the regenerative apparatus of this invention, enabling playback of the enciphered contents information which was recorded on record media,

such as DVD, only within the viewing-and-listening contract term of the contents information concerned based on the license information by which broadcast distribution is carried out cuts.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] Drawing having shown the example of a system configuration for offering the distribution-of-information service concerning the operation gestalt of this invention.

[Drawing 2] Drawing where contents information was recorded and in which having shown the example of a configuration of the record data of record media, such as DVD-ROM, for example.

[Drawing 3] Drawing having shown the example of a data configuration of license information.

[Drawing 4] Drawing having shown the example of a configuration of contract-management equipment.

[Drawing 5] Drawing having shown the example of a data configuration of User Information memorized by the contract user DB.

[Drawing 6] Drawing having shown the example of a data configuration of the information memorized by Seed DB.

[Drawing 7] Drawing having shown the example of a data configuration of the information memorized by the contents key DB.

[Drawing 8] The flow chart for explaining actuation of the contract-management equipment of drawing 4 .

[Drawing 9] Drawing having shown the example of a configuration of a regenerative apparatus.

[Drawing 10] Drawing having shown the example of a configuration of the license judging unit of drawing 9 .

[Drawing 11] The flow chart for explaining actuation of the regenerative apparatus of drawing 9 , and the license judging unit of drawing 10 .

[Drawing 12] The flow chart for explaining actuation of the regenerative apparatus of drawing 9 , and the license judging unit of drawing 10 .

[Description of Notations]

Broadcast management equipment

1 -- Contract user database

3 -- Seed database

4 -- Contents key database

5 -- License information database

8 -- License information generation section

9 -- License information generation control section

12 -- License information output request section

13 -- Broadcast equipment

14 -- Scheduling section

Regenerative apparatus

202 -- Filter

204 -- License information storage section

206 -- DVD drive

207 -- License information selection section

208 -- License judging unit
209 -- MPEG decoder
801 -- Master key generation section
802 -- Master key storing section
803 -- ID storing section
804 -- Decode section
805 -- Judgment section